

# STATEWIDE INFORMATION TECHNOLOGY INTERIM ARCHITECTURE

## **Interim Architecture Component: Wireless LAN (Local Area Network)**

**Short Title: Wireless LAN Architecture**

**Effective Date: October 10, 2006**

**Approved: Richard B. Clark**

### **I. Interim Architecture Purpose**

This document describes one component of the Network Architecture that will be developed by the Department of Administration Information Technology Services Division (ITSD). It lays out the technology used to provide wireless connectivity for entities using the State of Montana's SummitNet network.

### **II. Definitions**

Architecture: An architecture is a blueprint that defines the business, the information necessary to operate the business, the technologies necessary to support the business operations, and the transitional processes necessary for implementing new technologies in response to the changing business needs.

### **III. Closing:**

For questions on this interim architecture component, e-mail [ITpolicy@mt.gov](mailto:ITpolicy@mt.gov), or, contact the Information Technology Services Division at:

Chief Information Officer  
PO Box 200113  
Helena, MT 59620-0113  
(406) 444-2700  
FAX: (406) 444-2701

The technical contact at the Information Technology Services Division for this architecture is:

Steve Noland, Network Research and Design  
PO Box 200113  
Helena, MT 59620-0113  
(406) 444-2700  
FAX: (406) 444-2701

### **IV. Cross-Reference Guide:**

[ENT-SEC-012](#) – Internet/Intranet Security Policy

White Paper: [Wireless LAN \(Local Area Network\) Deployment Guide](#)

## V. Administrative Use:

History Log	
Approved Date:	
Effective Date:	
Change and Review Contact:	<a href="mailto:ITpolicy@mt.gov">ITpolicy@mt.gov</a>
Review:	Event Review: Any event affecting this policy may initiate a review. Such events may include a change in statute, key staff changes or a request for review or change.
Scheduled Review Date:	Three years from effective date or upon further development of Network Architecture
Last Review/Revision:	
Changes:	



Department of Administration  
Information Technology Services Division

## **Wireless LAN Architecture**

Date: 03/23/2006

## Table of Contents

<b>Section</b>	<b>Page Number</b>
1.0 Introduction	4
2.0 Wireless Technologies	6
2.1 WPA / WPA2	6
2.2 EAP	7
2.3 LEAP	7
2.4 PEAP	7
3.0 Hardware as Implemented	9
3.1 Wireless Access Points (AP)	9
3.2 Access Control Server (ACS)	9
3.3 Wireless LAN Access Solution Engine (WLSE)	9
3.4 Client Adapter (Supplicant)	10
3.5 Certificate Authority (CA)	10
3.6 Active Directory (AD)	10
4.0 Conclusion	11

## 1.0 INTRODUCTION

The Information Technology Services Division (ITSD) has deployed a wireless LAN solution allowing users to connect into the State of Montana's enterprise network, SummitNetII. This solution follows policy [ENT-SEC-012](#), Intranet/ Internet Policy.

There are two types of wireless users:

1. Secured users
2. Non-Secured users

Once the secured user has been authenticated and authorized onto the network, the user has full access to all resources within SummitNetII. The authentication and authorization process is described in section 2.0 Wireless Technologies. Policy ENT-SEC-012 states "All wireless connections to the inside (protected) portion of the network (inside) will be encrypted and authenticated". .

The non-secured user is neither authenticated or authorized and as such is not permitted any resources within SummitNetII secure network. The non-secure user is simply ported directly to the Internet upon completing registration.

The hardware platform solution for wireless is comprised of six parts:

1. Wireless Access Points (AP)
2. Access Control Server (ACS)
3. Wireless LAN Access Solution Engine (WLSE)
4. Client Adapter (Supplicant)
5. Certificate Authority (CA)
6. Active Directory (AD)

The Access Point is the device where clients attach with their radio signal using either 802.11A, 802.11B, or 802.11G. The access point bridges the radio signal to the hardwired Ethernet network.

The Access Control Server is used to authenticate, authorize and account (AAA) devices and users. This device uses the IETF standard of RADIUS as well as the Cisco proprietary TACACS+. The ACS server authenticates the users by accessing the enterprise Active Directory

(AD). At this time, the ACS server is to Authenticate, Authorize, and Account (AAA) wireless devices and users only. Eventually all network devices and users are to (AAA) through the ACS server. Non-secured users do not authenticate through ACS.

Wireless LAN access Solution Engine (WYLSE) is the management package that monitors and manages all of the APs.

Using this method of secured wireless access, only Cisco Systems, Inc client adapters are supported for the secured users at this time. The Cisco client adapters were selected due to signal strength and the availability of the Cisco extensions to aid in site surveys and the locating of rogue access points on the network. However all makes and models of client adapters are supported for the Internet only customer.

A central certificate authority is required to ensure ACS authentication. Authentication is accomplished by a server certificate located on each device, which authenticates ACS to the client. Non-secured client do not use the certificate server, nor do they have certificates.

Today existing network devices such as PC's, switches, and routers participate in the network by being physically connected via a cable; and as a result only the users are authenticated onto the network. Once wireless devices are allowed to participate in the network, the risk of unwanted devices is greatly increased. To avoid this, the device as well as the user must be authenticated. The technology deployed is based on the IEEE standard of 802.1X. 802.1X allows for secure device and user authentication. ITSD is installing a derivative of 802.1x, Wi-Fi Protected Access (WPA2). This allows for stricter encryption requirements using Advanced Encryption Standard (AES) which encrypts 128-bit blocks of data at a time with a 128-bit encryption key. WPA2 also allows for fast roaming, PMK caching, and pre-authentication.

Once a secured user or device is authenticated using the **enterprise** Active Directory (AD) the device is given its authorization information from the ACS server. This allows the user to automatically be placed in the correct VLAN for their work environment as well as access to the services they are granted regardless of where they are physically located. Non-secured users are not authenticated to the enterprise (AD).

## 2.0 WIRELESS TECHNOLOGIES

Non-secured users register themselves and accept the Internet acceptable use policy. The user is then granted access to a separate isolated secured, virtual network (VLAN) that is passed directly to the firewall and onto the Internet.

The non-secured client may use any supplicant and wireless card; configured for no authentication or encryption. The user connects to the SSID of guest. Once the wireless connection is established, the user opens up Internet Explorer and is redirected to the registration page. At this time the user provides contact information, and accepts the State of Montana's Internet Acceptable Use Policy.

All non-secured users are limited to a combined bandwidth to the Internet of 3Mb.

The guest Internet only VLAN is available Monday through Saturday from the hours of 5:00 AM until 10:00 PM.

It should be noted, users requiring access to the State of Montana's Intranet devices can do so from the non-secured wireless LAN SSID of guest. This would be accomplished by accessing a secure Citrix gateway or other approved VPN solution.

The remaining section discusses the technologies for secured users.

### 2.1 WPA / WPA2

WPA allows Temporal Key Integrity Protocol (TKIP) and message integrity check (MIC). Because the most popular attack against WEP relies on exploiting multiple weak initialization vectors in a stream of encrypted traffic using the same key, using different keys per packet is a potential way to mitigate the threat. The initialization vector and the WEP key are hashed to produce a unique packet key (called a temporal key) that is then combined with the initialization vector and run through a mathematical function called XOR with plain text. This prevents the weak initialization vectors from being used to derive the WEP. WPA allows for secure methods of authentication as discussed below.

WPA2 allows Advanced Encryption Standard (AES), which meets the Federal Information Processing Standard (FIPS) 140-2 requirement. Like WPA, WPA2 requires the determination of

a mutual pairwise master key (PMK) based on the EAP or PSK authentication processes and the calculation of pairwise transient keys through a 4-way handshake. WPA2 also requires support for the Advanced Encryption Standard (AES) using the Counter Mode-Cipher Block Chaining (CBC)-Message Authentication Code (MAC) Protocol (CCMP). AES Counter Mode is a block cipher that encrypts 128-bit blocks of data at a time with a 128-bit encryption key. The CBC-MAC algorithm produces a message integrity code (MIC) that provides data origin authentication and data integrity for the wireless frame. A Packet Number field included in the WPA2-protected wireless frame and incorporated into the encryption and MIC calculations provides replay protection.

WPA and WPA2 allow for secure methods of authentication as discussed on the following page. The three methods of authentication used in conjunction with 802.1x in use today are:

1. Extensible Authentication Protocol (EAP)
2. Protected Extensible Authentication Protocol (PEAP)
3. Cisco Wireless EAP (LEAP)

## 2.2 EAP

EAP authentication is the IETF RFC standard supported by the majority of wireless vendors and provides four significant benefits over basic 802.11 security.

1. The authentication scheme effectively eliminates "man-in-the-middle (MITM) attacks" introduced by rogue access points and RADIUS servers by requiring mutual authentication between client and RADIUS server.
2. Verifying the client, ACS, and radius credentials by use of certificates from a central certificate authority.
3. Centralized policy control such as session time out triggers, re-authentication and new key derivation by the use of certificates generated from a central authority.
4. Both the session key and broadcast key are changed at regular intervals as defined by the RADIUS server.

## 2.3 LEAP

LEAP is a Cisco proprietary authentication mechanism developed to augment EAP. LEAP relies on a shared secret, the user's logon password that is known by the client and the network. Client wireless cards other than Cisco cannot use this authentication.

## 2.4 PEAP

PEAP is an IETF draft RFC authored by Cisco Systems, Microsoft, and RSA security, and as such is due to become an open standard allowing for a variety of client wireless adapters. PEAP uses a digital certificate, which is generated from a central certificate authority for server authentication. For user authentication, PEAP encapsulates the packets within a protected Transport Layer Security (TLS) tunnel between the client and the server.

ITSD investigated all options of wireless technologies and selected WPA2 with PEAP as the preferred method for secure users.

## 3.0 HARDWARE

The hardware platform is based on five separate products that combine to form a cohesive wireless solution. Each hardware device and its function is described below.

### 3.1 Wireless Access Points (AP)

The Cisco Access point chosen for the wireless solution is the Aironet 1200 series. The Aironet 12xx supports simultaneous 2.4 GHz and 5 GHz radios while supporting IEEE 802.11b and 802.11g technologies, with the addition of an 802.11a radio card these access points can also support the IEEE 802.11a 5 GHz standard.

### 3.2 Access Control Server (ACS)

The Cisco ACS server is a rack-mounted, platform serving as a high performance access control server supporting RADIUS and TACACS authentication, accounting, and authorization (AAA). A primary and secondary ACS server combined with Active Directory (AD) provides a comprehensive AAA product solution. The AAA product is to be used to authenticate devices and users both wireless and wired.

The primary ACS server is located in Helena, and the failover unit is located in Billings.

Since users are currently sorted into user groups within AD, 802.1x can be implemented in stages based on these groups or by physical location, or by work group.

Non-secured users bypass the ACS server.

### 3.3 Wireless LAN Access Solution Engine (WLSE)

The WLSE is used to:

1. Manage and configure Cisco Wireless Access Points
2. Reports based on device tracking, client and security information
3. Fault and Policy Monitoring
4. Radio Management

Once building maps are imported into WLSE, radio quality can be managed and monitored.

### 3.4 Client Adapter

There are currently two models of client adapters supported for the secured and non-secured users:

1. 802.11b
2. 802.11g

As mentioned earlier the addition of a radio card would increase the support of the existing access points to include the IEEE standard for 802.11a.

The non-secured Internet only user can use any model laptop and client adapter. A standard default SSID of guest is used for these users to access Internet only VLAN.

The recommended software compatibility is a minimum of a laptop with Windows XP, Service Pak1, and patch 815485 with a client adapter that supports 802.1x. The Odyssey client software from Funk Software is the software chosen to manage the client adapters. This is the only combination that currently has been tested to support WPA2 with PEAP and certificates. Subsequent testing has proven Windows 2000 clients with 802.1x adapters and the Odyssey software also function in our wireless environment.

### 3.5 Certificate Authority (CA)

The ACS (Access Control Server) has been issued a certificate by the CA. This certificate is considered trusted and is loaded onto each client machine to ensure authentication requests are being sent to the correct ACS server.

### 3.6 Active Directory (AD)

The enterprise active directory is used by ACS to validate the username and password for secured wireless users only. Before an agency can begin adding users to the wireless network, the administrator must create a new group in active directory organizational unit. The naming convention is agencyname-secured-wireless. Once the new group has been created, the administrator can begin adding users. A userid is added to this new group and ACS will be able to authenticate and map them correctly.

Once the administrator has created the new group, the group needs to be mapped in ACS. To accomplish this, open a ticket with the helpdesk, to the network operations group.

## 5.0 CONCLUSION

ITSD investigated several variations of wireless technologies and selected WPA2 with PEAP as the preferred method for secure users. There is also a non-secured Internet only wireless network available.

In conclusion the Wireless LAN Deployment as designed and tested by ITSD in cooperation with Cisco Systems, Inc. is a secured, managed and monitored addition to the network in compliance with policy [ENT-SEC-012](#), Internet/ Internet Security Policy.